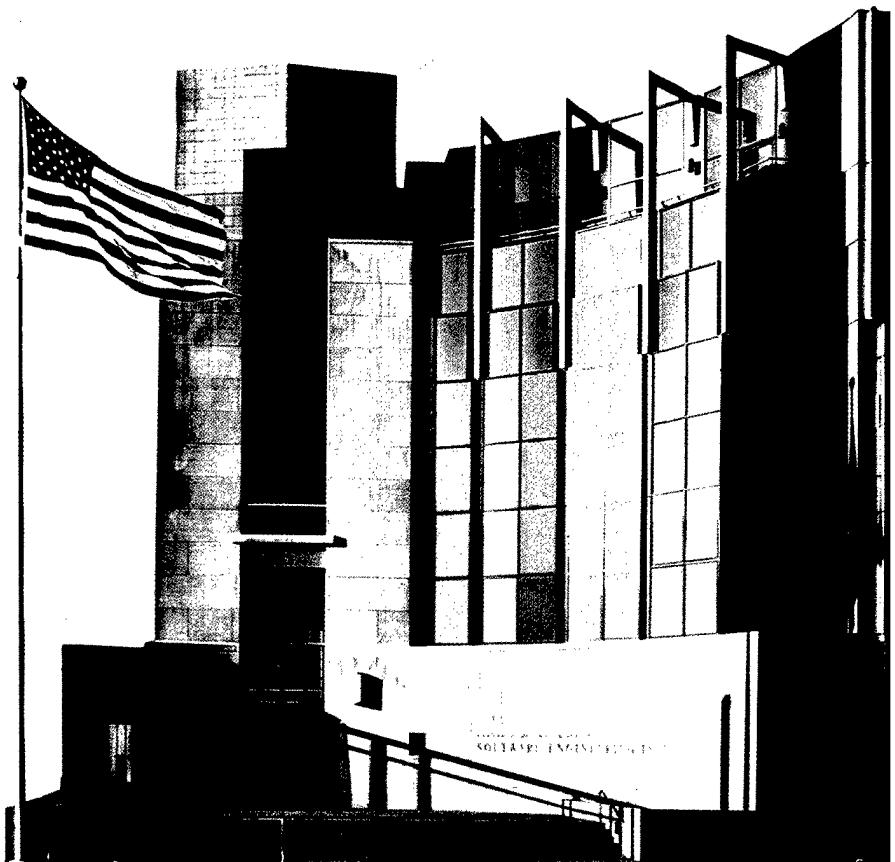
Carnegie Mellon
Software Engineering Institute

Responding to Intrusions

Klaus-Peter Kossakowski
Julia Allen
Christopher Alberts
Cory Cohen
Gary Ford
Barbara Fraser
Eric Hayes
John Kochmar
Suresh Konda
William Wilson

February 1999

SECURITY IMPROVEMENT MODULE
CMU/SEI-SIM-006



Carnegie Mellon University does not discriminate and Carnegie Mellon University is required not to discriminate in admission, employment, or administration of its programs or activities on the basis of race, color, national origin, sex or handicap in violation of Title VI of the Civil Rights Act of 1964, Title IX of the Educational Amendments of 1972 and Section 504 of the Rehabilitation Act of 1973 or other federal, state, or local laws or executive orders.

In addition, Carnegie Mellon University does not discriminate in admission, employment or administration of its programs on the basis of religion, creed, ancestry, belief, age, veteran status, sexual orientation or in violation of federal, state, or local laws or executive orders. However, in the judgment of the Carnegie Mellon Human Relations Commission, the Department of Defense policy of "Don't ask, don't tell, don't pursue" excludes openly gay, lesbian and bisexual students from receiving ROTC scholarships or serving in the military. Nevertheless, all ROTC classes at Carnegie Mellon University are available to all students.

Inquiries concerning application of these statements should be directed to the Provost, Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213, telephone (412) 268-6684 or the Vice President for Enrollment, Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213, telephone (412) 268-2056.

Obtain general information about Carnegie Mellon University by calling (412) 268-2000.

Carnegie Mellon
Software Engineering Institute
Pittsburgh, PA 15213-3890

Responding to Intrusions

CMU/SEI-SIM-006

Klaus-Peter Kossakowski
Julia Allen
Christopher Alberts
Cory Cohen
Gary Ford
Barbara Fraser
Eric Hayes
John Kochmar
Suresh Konda
William Wilson

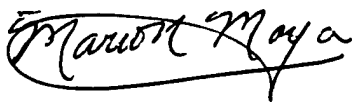
February 1999

Networked Systems Survivability Program

This report was prepared for the

SEI Joint Program Office
HQ ESC/DIB
5 Eglin Street
Hanscom AFB, MA 01731-2116

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.



Mario Moya, Maj, USAF
SEI Joint Program Office

This work is sponsored by the U.S. Department of Defense.

This work was created in the performance of Federal Government Contract Number F19628-95-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 52.227-7013.

This document is available through Asset Source for Software Engineering Technology (ASSET): 1350 Earl L. Core Road; PO Box 3305; Morgantown, West Virginia 26505 / Phone: (304) 284-9000 or toll-free in the U.S. 1-800-547-8306 / FAX: (304) 284-9001 World Wide Web: http://www.asset.com / e-mail: sei@asset.com

Copies of this document are available through the National Technical Information Service (NTIS). For information on ordering, please contact NTIS directly: National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161. Phone: (703) 487-4600.

This document is also available through the Defense Technical Information Center (DTIC). DTIC provides access to and transfer of scientific and technical information for DoD personnel, DoD contractors and potential contractors, and other U.S. Government agency personnel and their contractors. To obtain a copy, please contact DTIC directly: Defense Technical Information Center / Attn: BRR / 8725 John J. Kingman Road / Suite 0944 / Ft. Belvoir, VA 22060-6218 / Phone: (703) 767-8274 or toll-free in the U.S.: 1-800 225-3842.

Table of Contents

Preface iii

Responding to Intrusions 1

1. Establish policies and procedures for responding to intrusions. 7
2. Prepare to respond to intrusions. 11
3. Analyze all available information to characterize an intrusion. 17
4. Communicate with all parties that need to be made aware of an intrusion and its progress. 23
5. Collect and protect information associated with an intrusion. 27
6. Apply short-term solutions to contain an intrusion. 31
7. Eliminate all means of intruder access. 35
8. Return systems to normal operation. 39
9. Identify and implement security lessons learned. 43

Preface

This document is one of a series of publications of the Software Engineering Institute at Carnegie Mellon University called *security improvement modules*. They are intended to provide practical guidance to help organizations improve the security of their networked computer systems.

Module structure

Each module addresses an important but relatively narrowly defined problem in network and system security. The first section of the module describes the problem and outlines a set of *security improvement practices* to help solve it. Each practice is a recommended way of performing common tasks related to the secure operation of networked computer systems.

The remaining sections of the module are detailed descriptions of the practices. Each includes a rationale for the recommended actions and a description of how to perform them.

Intended audience

The practices are primarily written for system and network administrators whose day-to-day activities include installation, configuration, and maintenance of the computers and networks. Occasionally, practices are written to assist the managers responsible for network and system administration.

Revised versions

Network and system technologies continue to evolve rapidly, leading to new security problems and solutions. Modules and practices need to be revised occasionally, so to permit more timely publication of new versions, we also publish them on the World Wide Web. At the end of each section of this document is the URL of its Web version.

Implementation details

How an organization adopts and implements the practices often depends on the networking and computing technologies it uses. For some practices, technology-specific implementation details are published on the World Wide Web. The Web version of each practice contains links to the implementation details.

Responding to Intrusions

Most organizations are not adequately prepared to deal with intrusions. They are likely to address the need to prepare and respond only after a breach occurs. The result is that when an intrusion is detected, many decisions are made in haste and can reduce an organization's ability to

- understand the extent and source of an intrusion
- protect sensitive data contained on systems
- protect the systems, the networks, and their ability to continue operating as intended
- recover systems
- collect information to better understand what happened. Without such information, you may inadvertently take actions that can further damage your systems.
- support legal investigations

Even if you have sophisticated prevention measures in place, intrusions can happen. In this module, we describe practices to be implemented independent of the size, type, or severity of an intrusion or of the methods used to gain access. The key event is that an intruder has gained access to your systems or data.

You need a strategy for handling intrusions effectively that includes preparation, detection, and response. The practices in this module identify steps you must take to respond to and recover from a detected intrusion.

This module is a companion module to CMU/SEI-SIM-005 *Preparing to Detect Signs of Intrusion* and CMU/SEI-SIM-001 *Detecting Signs of Intrusion.*

Who should read these practices

These practices are intended primarily for system and network administrators, managers of information systems, and security personnel responsible for networked information resources.

These practices are applicable to your organization if your networked systems infrastructure includes

- host systems providing services to multiple users (file servers, timesharing systems, database servers, Internet servers, etc.)
- local-area or wide-area networks

- direct connections, gateways, or modem access to and from external networks, such as the Internet

We recommend that you read all of the practices in this module before taking any action. To successfully implement the practices, it is important that you understand the overall context and relationships among them. For instance, once you read the practices in the Handle category, it is easier to understand the Practices in the Prepare category (see the Summary of Recommended Practices table on page 4).

If you are dealing with an intrusion, you may want to skip the first two preparatory practices and move immediately to Practice 3, "Analyze all information necessary to characterize an intrusion." Once you have completed your response and recovery process, we recommend that you review and implement the preparatory practices.

What these practices do not cover

These practices do not address

- preparing to detect signs of intrusion or detecting signs of intrusion. For guidance on these topics, see *Preparing to Detect Signs of Intrusion* [Kochmar 98] and *Detecting Signs of Intrusion* [Firth97a].
- securely configuring your workstations and servers. For guidance on these topics, see *Securing Desktop Workstations* [Simmel 99] and *Securing Network Servers* [Ford 99].
- responding to incidents that are not intrusions, including the analysis and characterization of such incidents
- dealing with intruder attempts to find out about your system using probes, scans, and other types of mapping methods
- responding to denial of service attacks

Security issues

Intruders are always looking for ways to break into systems. For example, they may attempt to breach your network's perimeter defenses from external locations, or physically infiltrate your organization to gain internal access to its information resources. They may want to access your organization's network to hide their identity and to launch an attack on another site.

Intruders seek and take advantage of newly discovered vulnerabilities in operating systems, network services, and protocols. They actively develop and use sophisticated programs to rapidly penetrate systems. As a result, intrusions, and the damage they cause, are often achieved in a matter of seconds.

You will not know what to do in the event of an intrusion if the necessary procedures, roles, and responsibilities have not been ***defined and exercised in advance.*** The absence of systematic and well-defined procedures can lead to

- extensive damage to data, systems, and networks due to not taking timely action to contain an intrusion. This can result in increased costs, loss of productivity, and loss of business.
- the possibility of an intrusion affecting multiple systems both inside and outside your organization because staff did not know who else to notify and what additional actions to take
- negative exposure in the news media that can damage your organization's stature and reputation with your shareholders, your customers, and the community at large
- possible legal liability and prosecution for failure to exercise an adequate standard of due care when your systems are inadvertently or intentionally used to attack others

Security improvement approach

The order in which practice steps are to be executed and time relationships among practices are shown in the diagram below. An intrusion occurs at time "T1" and the response process is complete at time "Tn."

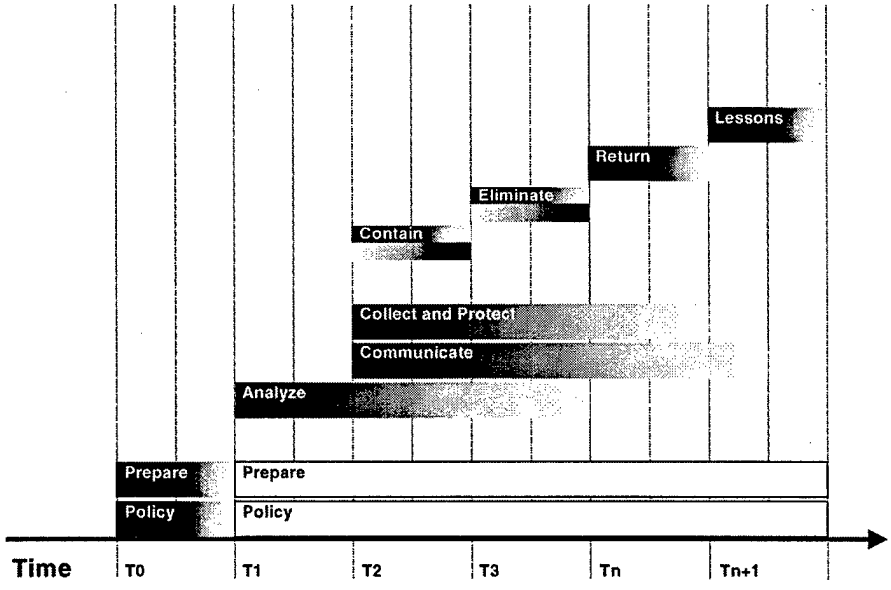
Practice titles are abbreviated in this description. The full titles can be found in the Summary of Recommended Practices table below.

The steps in the Policy and Prepare practices help you prepare to respond to an intrusion. Ideally, you should implement them prior to exposing your networks and systems to intruders. You can implement them any time during or after a response process execution, except when the compromised status of systems involved in an intrusion prevents you from taking recommended preparation actions. You should examine and exercise the steps called out in these two practices on an ongoing basis as tools, methods, policies, and procedures change.

At time T1, you need to execute the steps in the Analyze practice. Once some initial analysis is completed, you then execute the steps in the Communicate and Collect and Protect practices. From this point in time forward (T2), the steps in the Analyze, Communicate, and Collect and Protect practices occur throughout the process and should be executed in parallel as events dictate.

You execute the steps in the Contain practice after initial analysis is complete and then iteratively with the steps in the Analyze practice. You execute the steps in the Eliminate practice after the first round of containment actions occur and then iteratively with further Analyze and Containment actions.

Ideally, you perform the steps in the Return practice after the Eliminate steps are complete. And the steps in the Lessons practice should take place shortly after returning your systems to normal operation.



To reflect this set of practice relationships, we group the nine practices into three categories

- preparing to respond to intrusions
- handling an intrusion
- taking necessary follow-up steps to ensure that your security practices are improved. This will result in a more secure operational environment that is based on what you learned as you responded to an intrusion.

Summary of recommended practices

Category	Recommended Practice
Prepare	1. Establish policies and procedures for responding to intrusions. 2. Prepare to respond to intrusions.
Handle	3. Analyze all available information to characterize an intrusion. 4. Communicate with all parties that need to be made aware of an intrusion and its progress. 5. Collect and protect information associated with an intrusion. 6. Apply short-term solutions to contain an intrusion. 7. Eliminate all means of intruder access. 8. Return systems to normal operation.
Follow up	9. Identify and implement security lessons learned.

Abbreviations used in these practices

CEO	Chief Executive Officer
CIO	Chief Information Officer
CSIRT	Computer Security Incident Response Team
DNS	Domain Name System
FIRST	Forum of Incident Response Security Teams
FTP	file transfer protocol
HTTP	hypertext transfer protocol
IP	Internet Protocol
ISP	Internet Service Provider
NTP	Network Time Protocol
SATAN	System Administrator Tool for Analyzing Networks
SMTP	simple mail transfer protocol
TCP	transmission control protocol
WORM	Write Once, Read Many
WWW	World Wide Web

Definitions used in these practices

artifact	instances of malicious code or other file remnants left behind by intruders. Examples include Trojan horse programs, Ethernet sniffer log files, password files, exploit scripts, and other program source code [West-Brown 98].
attack	a series of steps taken by an attacker to achieve an unauthorized result [Howard 98]; any attempt to gain knowledge of or penetrate a

	system; includes scanning, probing, mapping, and all adverse events described under incident [Schultz 98]
breach	same as intrusion
chain of custody	verifiable documentation that indicates the sequence of individuals that have handled a piece of evidence and the sequence of locations where that evidence has been stored, including dates and times. For a proven chain of custody to occur, the evidence is accounted for at all times.
contingency plan	documentation describing the actions needed to allow business operations to continue if primary facilities, personnel, systems, networks, etc. are unable to operate. A contingency plan is most commonly put into effect during events such as power outages, unexpected system shutdowns, fires, and other natural disasters.
event	an action directed at a target which is intended to result in a change of state (status) of the target [Howard 98]
incident	any real or suspected adverse event in relation to the security of computer systems or computer networks. Examples of such events include intrusion via the network, the occurrence of computer viruses, and probes for vulnerabilities via the network to a range of computer systems (often referred to as scans) [West-Brown 98]
incident handling	actions taken to protect and restore the normal operating condition of computers and the information stored in them when an adverse event occurs; involves contingency planning and contingency response [Schultz 98]
incident response	same as incident handling
intrusion	any intentional event where an intruder gains access that compromises the confidentiality, integrity, or availability of computers, networks, or the data residing on them [SEI 99]
sniffer	any hardware or software device that monitors network traffic. The traffic can be stored and archived for later viewing. Intruders commonly use sniffers to capture user id and password data that are passed in clear text over a network.

References

[CERT 98] *Steps for Recovering from a UNIX Root Compromise*. Available at http://www.cert.org/tech_tips/root_compromise.html.

[Firth 97a] Firth, Robert, et al. *Detecting Signs of Intrusion.* (CMU/SEI-SIM-001, ADA329629). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1997. Available at http://www.cert.org/security-improvement/modules/m01.html.

[Firth 97b] Firth, Robert, et al. *Security for a Public Web Site.* (CMU/SEI-SIM-002, ADA329626). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1997. Available at http://www.cert.org/security-improvement/modules/m02.html.

[Ford 99] Ford, Gary, et al. *Securing Network Servers.* (CMU/SEI-SIM-007). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1999. [to be published]

[Howard 98] Howard, John. Longstaff, Tom. *A Common Language for Computer Security Incidents.* (SAND98-8997). Albuquerque, NM: Sandia National Laboratories, 1998.

[IETF 97] Internet Engineering Task Force Network Working Group. *RFC 2196 Site Security Handbook.* Edited by Barbara Fraser. Available online at ftp://ftp.isi.edu/in-notes/rfc2196.txt (1997)

[Kochmar 98] Kochmar, John, et al. *Preparing to Detect Signs of Intrusion.* (CMU/SEI-SIM-005). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1998. Available at http://www.cert.org/security-improvement/modules/m05.html.

[Maiwald 98] Maiwald, Eric. *Automating Response to Intrusions.* The Fourth Annual UNIX and NT Network Security Conference. Orlando, FL: The SANS Institute, October 24-31, 1998.

[Marchany 98] Marchany, Randy. *Incident Response: Scenarios and Tactics.* The Fourth Annual UNIX and NT Network Security Conference. Orlando, FL: The SANS Institute, October 24-31, 1998.

[Northcutt 98] Northcutt, Stephen. *Computer Security Incident Handling: Step-by-Step.* The Fourth Annual UNIX and NT Network Security Conference. Orlando, FL: The SANS Institute, October 24-31, 1998.

[Simmel 99] Simmel, Derek, et al. *Securing Desktop Workstations.* (CMU/SEI-SIM-004). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1999. [to be published]

[SANS 98] *Computer Security Incident Handling Step By Step Guide, v1.5.* The SANS Institute. May, 1998.

[Schultz 98] Schultz, Eugene. *Effective Incident Response.* The Fourth Annual UNIX and NT Network Security Conference. Orlando, FL: The SANS Institute, October 24-31, 1998.

[SEI 99] *Protecting Taxpayer Information: Detecting Intrusions Instructor's Guide.* Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1999.

[West-Brown 98] West-Brown, Moira. Kossakowski, Klaus-Peter. Stikvoort, Donald. *CSIRT Handbook.* (CMU/SEI-98-HB-001). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1998. Available at http://www.sei.cmu.edu/publications/documents/98.reports/98hb001/98hb001abstract.html.

Where to find updates

The latest version of this module is available on the Web at URL

http://www.cert.org/security-improvement/modules/m06.html

1 *Establish policies and procedures for responding to intrusions.*

A security policy defines the rules that regulate how your organization manages and protects computing resources to achieve security objectives. For responding to intrusions, one of the policy's primary purposes is to document the threats you intend to guard against and the actions you intend to take in response to a successful attack.

Response procedures describe how the response policies will be implemented throughout your organization, e.g., who to notify, at what point in the response procedure, and with what types of information. From these procedures, all concerned parties are able to determine what operational steps they need to take to comply with your policies and, thereby, respond in a manner that upholds the security objectives for your organization's information and networked systems.

This practice describes a subset of the topics your intrusion response policies and procedures should address. Additional policy and procedure information is contained in the other practices of this module where it is most applicable. This language needs to be tailored to reflect the specific business objectives and security requirements of your organization and its computing environment. The details of procedures used to address specific types of intrusions may vary.

Why this is important

Policies and supporting procedures that are documented, communicated, and enforced prepare you to respond to intrusions in a timely, controlled manner. This gives you the ability to exercise your procedures and eliminate potential errors or omissions in advance of an intrusion. During or after an attack on your system, you do not want to be in a position of needing to determine what actions to take, what data to gather and preserve, and how to protect your data, systems, and networks from further damage.

Having documented plans, conducted training, and tested procedures in advance will allow staff members to efficiently coordinate their activities when responding to an intrusion. Without the knowledge conveyed through training and test exercises, users may inadvertently expose parts of the organization to security threats. For example, users might reveal sensitive information if they contact the wrong person when observing an intrusion.

How to do it

Note that we use the verb "document" in the steps below to include both the creation of specific information and the recording of it in a form that can be used as a reference.

➤ *Establish guidelines and rules at the management level for responding to intrusions and include these in your organization's networked systems security policy.*

These guidelines and rules can be categorized as follows:

Priority and sequence of actions

Document the priority and sequence of actions to be taken when dealing with an intrusion. Actions necessary to protect human life and safety are likely to have priority over those that ensure operational continuity, protect classified and sensitive data, or prevent damage to systems. Document the criteria by which the priority and sequence of actions can change

- over time
- as you obtain additional information (such as the extent of an intrusion)
- as you become aware that an intrusion you are analyzing interacts with one or more other intrusions.

Actions to be taken can include

- denying access to an intruder, possibly by disconnecting the affected system from the network and shutting down the system
- containing an intrusion and limiting the actions of an intruder
- continuing operation to gather additional information
- restoring the affected system. You need to specify the order in which services will be restored, if this is a consideration (for example, restore your e-mail service before restoring ftp). This ensures that the order meets your business objectives and priorities while minimizing negative effects on users, when possible.

Authority to act

This policy should indicate what types of intrusion response actions require management approval and which are pre-approved.

Document the circumstances under which you intend to

- stay connected to pursue an intruder by gathering additional information
- protect your systems by disconnecting and shutting down
- conduct covert monitoring of network traffic and file access

Ensure that the individuals or team responsible for intrusion response have pre-authorization from management to disconnect from the network and shut down the affected system(s), if appropriate. This will cause a denial of service condition on the affected system until it is returned to operation.

Document the actions to be taken in dealing with intrusions involving remotely connected computers used by your employees and vendors if these actions differ from those taken for other types of intrusions.

Intrusion response resources

Determine how you will structure and staff your intrusion response activity. One option is to create a computer security incident response team (CSIRT). For this option, determine if the team will be distributed or centralized and identify the roles to be filled by team members based on your organization's security policies and procedures. Identify qualified people to assume these roles and determine how much of their time will be devoted to team activities. Ensure that you have a knowledgeable team trained and in place to handle

the full intrusion response and recovery process.

Refer to the *CSIRT Handbook* [West-Brown 98] for more information on this subject, including a full range of procedures to consider when operating such a team.

If you choose not to create a CSIRT, ensure that all response roles and responsibilities are clearly assigned to system and network administrators, security personnel, and other staff.

➤ *Document your configuration redundancy policy.*

If a critical machine is compromised as a result of an intrusion, having redundant equipment in place enables you to restore service quickly while preserving all of the evidence on the compromised machine and to perform ongoing analysis. You need to describe, for example, where and when to use hot, warm, and cold backups[1].

Ensure that this policy is consistent with your business continuity policy.

➤ *Document a response procedure that implements your intrusion response policies.*

Steps in such a procedure include

- analyzing all available information to characterize an intrusion, including assessing the damage and extent of an intrusion and an intruder's activities.
- communicating with all parties that need to be aware of an intrusion and participate in handling it, taking into account that an intruder may be able to access and monitor your means of communication.
- collecting and protecting information associated with an intrusion.
- containing an intrusion and determining what actions to take.
- eliminating an intruder's means of access and any related vulnerabilities.
- returning your systems to normal operation.
- following up including performing a post mortem review of events as they occurred and reviewing your policies and procedures

Document the roles, responsibilities, and authority of all staff involved in executing this procedure. Identify who performs each activity, when, and under what conditions.

Ensure that your intrusion response procedure is consistent and integrated into your business continuity and disaster recovery processes.

➤ *Conduct a legal review of your policies and procedures.*

This should be performed by your organization's legal counsel or a knowledgeable attorney you trust. The legal review should ensure that your policies and procedures

- are legally defensible and enforceable
- comply with overall company policies and procedures
- reflect known industry best practices demonstrating the exercise of due care

---

1. Hot backups provide the capability to immediately switch configurations as the backup system is being run in parallel with the primary system. Warm backups require some degree of reconfiguration before being used since they are not run in full parallel with operational systems. Cold backups need to be started from a shutdown state and brought up to date before being used.

- conform to national, state, and local laws and regulations
- protect your staff from lawsuits
- protect your organization from being held legally responsible in the event of a compromise. This part of the review should include a consideration of the legal implications of continuing to allow intruders access as you gather additional information about their activities. The risk is that they might continue to use your system to attack others.

Ensure that your legal counsel knows

- when to prosecute and what should be done to prosecute an intruder
- procedures that should be included to protect privacy
- procedures that should be included to ensure the admissibility of evidence
- when to report an intrusion to local, state, or national law enforcement agencies

➤ *Train designated staff about your response policies and procedures.*

During the training process, users should learn

- how to communicate appropriately with the news media including forwarding inquiries to your organization's public relations staff
- the actions they need to take to report a suspected intrusion, including who to notify, how (web, e-mail, phone), and what information they should report
- the use of intrusion response tools and environments based on their roles and responsibilities

Create and conduct periodic training about your response policies and procedures. This training should be mandatory for all new employees and should review specific policies and procedures relevant to the employee's knowledge and responsibilities.

Test the effectiveness of the training and each employee's readiness. Conduct practice drills (e.g., responding to break-ins and viruses) that test procedures and execute operational activities, making sure all staff members are aware of their roles and responsibilities. Conduct post-mortem meetings with trainees. Provide remedial training as required.

Regularly conduct mandatory security awareness refresher training for designated staff. Highlight recent changes to policies or procedures and summarize recent incidents and intrusions. Make this subject a recurring topic at executive and management-level staff meetings to maintain awareness.

Obtain information from the FBI and local law enforcement about preserving the chain of custody for evidence. Ensure that your system and network administrators, intrusion response staff, and their managers are aware of this information.

To stay current with the fast rate of technological change, ensure that system and network administration staff set aside time to maintain and update the knowledge and skills they need in technical topics required to implement your policies and procedures.

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at URL

http://www.cert.org/security-improvement/practices/p044.html

2 *Prepare to respond to intrusions.*

Preparation includes selecting, installing, and becoming familiar with tools that will assist you in the response process and will help you collect and maintain data related to an intrusion. You need to perform these preparation steps well in advance of an intrusion.

You need to understand and know how to use a range of tools to support your response procedures, including

- tools that capture data, configurations, backups, and cryptographic checksums about the systems involved in an intrusion. The outputs produced by these tools help you to analyze the system and provide information for system recovery.
- tools and data that directly support your response procedures, such as an isolated computer system to test artifacts that were found on compromised systems, and a contact database for those you need to keep informed about an intrusion.

You need to ensure all tools and related data are available, taking into account that the systems involved in an intrusion may not be working reliably or may not be available until an intrusion is contained and the recovery is successfully accomplished. This may require that you make additional systems available for tool execution or that you take additional steps to ensure that your tools are reliable and can be executed securely on the compromised system.

Why this is important

You will not be able to respond to an intrusion efficiently if you do not have the appropriate tools and data available prior to detecting an intrusion.

If you lack the necessary tools and data, you are likely to enact your response procedures later than desired, potentially increasing the extent and damage of an intrusion. This can make recovery more difficult. If you wait until an intrusion occurs to identify and install needed tools, you may not be able to obtain a working version of the tools in the required time period. This can make it difficult to create the correct set of data you need for tool execution. Analysis results that would help you clarify your current situation may not be available. You may not be able to restore a compromised system to its previous operational state if trusted backups are not accessible.

Tools may not operate predictably and effectively if they are not kept up to date. Tools may not operate reliably if they are not protected to ensure their authenticity and integrity. Their results could have been manipulated to hide signs of an intrusion. If they are not protected to ensure their availability, you will not be able to access them to assist you in your response procedures.

How to do it

➤ *Build an archive of boot disks and distribution media for all applications and all operating systems and versions.*

Having an archive of original or trusted boot disks (or CD-ROMs) provides the capability to restart a specific computer from a known, preexisting configuration. This ensures, to a large extent, that compromised files, programs, and data are not reloaded onto the system.

There are often incompatibilities in different operating system versions that may preclude, for example, full access to systems disks. Therefore, it is important to have all operating system versions in the archive to successfully rebuild your system and to include the original distribution media for each. Having this information allows you to

- reinstall a specific version of the operating system, when necessary
- install the trusted version on a test machine and compare files (trusted vs. installed, possibly compromised) for unexpected changes

All media should be hardware-write-protectable to avoid intentional or inadvertent tampering.

➤ *Build an archive of security-related patches for all applications and all operating systems and versions.*

Every new version of every operating system or application contains some unknown vulnerabilities and errors. Vendors provide security-related patches (also called bug-fixes, hot-fixes, etc.) to correct these. Usually they provide such patches free of charge to their customers.

Having an archive of patches allows you to initiate a specific operating system or application in a known, secure configuration by applying patches whenever the software is initially installed or subsequently reinstalled.

➤ *Identify and install tools that support the reinstallation of systems, applications, and patches.*

This includes

- installation servers containing trusted, generic versions of the original distribution for all operating systems, applications, and versions. The reinstallation process can be executed from these servers for a network with a large number of hosts with prompting for any host-specific information such as IP address.
- all tools that are needed to retrieve, unpack, verify, and install software patches that are intended to correct errors and eliminate vulnerabilities

Refer to the practice "Keep operating systems and applications software up to date" for more information in *Securing Desktop Workstations* [Simmel 99].

➤ *Ensure that your backup procedures are adequate to recover from any damage.*

During daily operations, the generation of backups provides you with copies of the system and its data. You depend on these copies to be able to restore the most recent version of the system or specific data files in the event of damage to your systems or data. You need to have high confidence that the restored assets are as you intended by regularly testing your ability to restore these assets from previously stored backups.

Also refer to the practice "Configure computers for file backups" in *Securing Desktop Workstations* [Simmel 99].

➤ *Build an archive of test results that describe the expected state of your systems.*

We recommend that you prepare a set of test results to use for comparison purposes. This will allow you to have some level of confidence that your systems have been properly restored after an intrusion occurs. Such results may include a scan for services on the network level (building up an authoritative list of such services) and a file of cryptographic checksums for critical configuration files (building up an authoritative list of such checksums).

➤ *Ensure that high capacity, removable- and hardware-write-protectable media and supporting equipment are available to make and restore system backups.*

Backups made during the response process are used

- to save the latest version of data and configuration information. This is necessary for restoring systems to their last known state, which will include the most recent modifications made by users and system administrators not available from the routine backups.
- to ensure that evidence on compromised systems is preserved
- to provide an easy way to establish the compromised environment on other systems required to conduct analysis (for example, on an isolated test network)

The media that you use to store backups must have sufficient capacity to contain all backup information.

To make backups and to load backups on other systems, all of the necessary devices, cables, plugs, and terminators need to be available as well as the software that was used to create the backups.

If possible, use media that cannot be written again once it has been used (i.e., protected for read only access such as WORM media). This safeguards the information and avoids accidental overwriting.

➤ *Build and maintain a database of contact information.*

The database should contain contact information for all individuals and organizations called out in your information dissemination policy and procedure. (Refer to the practice "Communicate with all parties that need to be made aware of an intrusion and its progress.") This includes response teams within your organization and those that operate nationally and internationally (refer to Other information below) as well as your public relations and legal staff.

Design the contact database so that it can be easily accessed and updated. Keep all contact information up to date.

To ensure database availability during an intrusion, store a backup copy off-site, have a copy available on an accessible system that is not connected to any network such as a laptop, and have hardcopies available.

Having access to a trusted version of your contacts database is critically important when you need to communicate with those involved. Protect the database as you would any other type of critical information. It can reveal a great deal about how you conduct your response process.

➤ *Set up secure communication mechanisms.*

You need to determine with whom you will need to communicate using secure mechanisms during the handling of an intrusion. Communication may take place using electronic

means such as email. All points of contact need to agree on what technology to use and exchange authenticated encryption and signature keys in advance. You may want to consider protecting other communication mechanisms such as fax or phone using encryption technology.

Be aware that even the act of two people communicating could indicate to an intruder that they have been detected. A sudden flurry of encrypted email from your internal security group to users, system administrators, CSIRTs, and others is a sure sign that something is happening. Your response procedures need to take this into account including the possibility of conducting all communications without use of email (e.g., using only phone and fax).

If you depend on secure communication mechanisms that use encryption, you need to manage all keys and authenticate those keys. This includes verifying that the keys belong to the identified point of contact and are not compromised prior to or during key exchange. If you are dealing with a large number of contacts, exchanging and authenticating keys can be quite burdensome. You may want to take advantage of commercial certificate authorities (CAs) to certify keys for all points of contacts or, at least, those outside of your organization.

In the event that you cannot communicate via the Internet or your organization's intranet, ensure that you establish alternate paths for communication with critical sites such as phone lines with direct modem connections.

➤ *Identify and install tools to access directories and other sources of contact information.*

Not all contact information can be derived prior to the occurrence of an intrusion. If an intrusion originates from an Internet host, you will need to search for the appropriate contacts for that host. Directories such as "whois"[1] or DNS (Domain Name System) provide information about organizations that are present on the Internet.

Various telephone directories are also present on the Internet. These can be accessed using Web browsers or with tools targeted for specific databases.

Tools that access these sources of information need to be included in the resource kit described in the next step.

➤ *Build a resource kit of tools and hardware devices.*

The resource kit should contain all tools that you may need to use in the response process. Examples of such tools include those that make and restore backups, compare files, build and compare cryptographic checksums, take system snapshots, review system configurations, list services and processes, trace the path to the attacking site and their ISP, etc.

Ensure that the resource kit is available on clean, hardware-write-protectable media.

Ensure that hardware devices such as printers or laptops are reserved for use in the event of an intrusion. Hardcopy materials are often required as part of an intrusion log and archives. For example, laptops can be used to monitor your network for suspicious activity, to retrieve contact information from Internet directory servers, and to access previously collected information such as default configurations and user id lists.

1. Refer to http://rs.internic.net/tools/whois.html

➤ *Ensure that test systems and networks are properly configured and available.*

Using compromised systems for any kind of analysis or test may expose these systems to further damage and, given the systems have been compromised, any results produced by them are unreliable. In addition, using such systems may inadvertently inform an intruder of the tests you are executing through the generation of network messages by malicious or compromised programs.

We recommend that you use test systems and test networks that are both physically and logically separated from any operational system and network. If you have sufficient resources available, you may choose to move the compromised systems to a test network and deploy newly installed and fully patched and secured systems so as to continue operations. Newly installed systems may have the same vulnerability that an intruder used to gain access. However, making the original systems available for analysis may give you an advantage over other approaches for reconstituting the compromised systems on your test network. In addition, the newly installed system will not contain any software that the intruder may have left behind.

If your equipment is limited or you do not want equipment to be idle when no analysis is being performed, you may choose to have a plan and process in place to configure a test environment quickly, on an as-needed basis.

After analysis is complete, clear all disks to ensure that any remnant files or malicious programs do not impact future analysis, any ongoing work on the test system, or are inadvertently transferred to other operational systems. This is particularly critical in the event that your test system is used for other purposes.

Make a backup of all analyzed systems to protect the results of your analysis in the event you need to do further analysis in the future.

Policy considerations

Your organization's networked systems security policy should

- require that designated system and network administrators, and response team members are trained in the use of intrusion response tools and environments. This training should include participation in response practice drills or simulations using the tools and environments.
- require that the inventory of all applications software, operating systems, supporting tools, and hardware be kept up to date.
- require quick access to backups in an emergency, even if they are stored at a remote site. This may include defining procedures that give specific managers the responsibility to authorize such access.
- state that staff members dealing with an intrusion may need to gain access to restricted systems and data. This may include
  - specifying how staff access is granted and how they will obtain administrator passwords and encryption keys
  - establishing the authority for staff access
  - establishing the authenticity of the staff member obtaining access
  - requiring that all access is documented and tracked

Other information

The Forum of Incident Response and Security Teams (FIRST) brings together a variety of computer security incident response teams from government, commercial, and academic

organizations. FIRST aims to foster cooperation and coordination in incident prevention, to prompt rapid reaction to incidents, and to promote information sharing among members and the community at large.

The goals of FIRST are

- to foster cooperation among information technology constituents in the effective prevention, detection, and recovery from computer security incidents
- to provide a means for the communication of alert and advisory information on potential threats and emerging incident situations
- to facilitate the actions and activities of the FIRST members including research, and operational activities
- to facilitate the sharing of security-related information, tools, and techniques

Currently, FIRST has 70 members.

Contact information for FIRST teams can be obtained from http://www.first.org/team-info.

For additional preparation practices, refer to *Preparing to Detect Signs of Intrusion* [Kochmar 98].

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at URL

http://www.cert.org/security-improvement/practices/p045.html

3 *Analyze all available information to characterize an intrusion.*

Once you have been alerted by your intrusion detection mechanisms or another trusted site that an intrusion has been detected, you need to determine to what extent your systems and data have been compromised and you need to respond. Information, as collected and interpreted through analysis, is key to your decisions and actions throughout the response process.

The purpose of analysis is to find out

- what attacks were used to gain access
- what systems and data were accessed by an intruder
- what an intruder did after obtaining access
- what an intruder is currently doing when an intrusion has not been contained or eliminated

You may be notified by other organizations that they have found evidence (such as a log file produced by an intruder tool that shows all successful connections) that your systems were attacked from their systems, or attacks on their systems were detected as originating from your systems. You may also receive such a report from a response team that coordinates the response effort of affected sites.

During the analysis, you may be tempted to actively collect additional information about the systems an intruder used to attack your systems. Such attempts can alert an intruder to your activities. In the event where the attacking system belongs to another organization, active data collection may itself be interpreted as intruder activity.

Therefore, the value of collecting as much information as possible needs to be balanced against the possible risk of intruders recognizing that their activities have been detected. Some intruders may panic and attempt to delete all traces of their activities, further damaging the systems you are trying to save. Others may not return, in which case any follow-up information you planned to collect the next time they entered your system will not be obtained.

This practice assumes you have previously performed the steps identified in *Preparing to Detect Signs of Intrusion* [Kochmar 98] and *Detecting Signs of Intrusion* [Firth 97a].

Why this is important

In order to deal with an intrusion effectively, you need to determine its scope and impact and prioritize your intended actions. This is possible only when you have analyzed all available information. For example, your actions may depend on the level of access an intruder gained and how confident you are that your analysis of the intruder's access level is correct.

How to do it

➤ *Capture and record system information that may be lost or not captured during the execution of your backup procedure.*

This includes

- all current network connections
- all current processes
- active users currently logged on
- all open files (files may be deleted if a process exits when the network is disconnected)
- any other volatile data that would be lost such as memory or cache

➤ *Backup the compromised systems.*

Make at least two full backups of the system or systems that have been identified as compromised as well as the user data on those systems. Do so using hardware-write-protectable or write-once media.

Preserve the backup media in a secure location. They may be reinstalled on other test systems for further analysis and the data may be used for system recovery.

To protect the backup as evidence, preserve the second backup media in a secure location and preserve the chain of custody. Do not use this copy for any operational task.

In specific instances or for critical environments, the backups are used to reinstall the compromised system on other hosts and hard drives while the original hosts and hard drives are preserved as evidence. This approach preserves the original environment most accurately even though it may alert an intruder and require significant hardware resources.

Be aware of the following and plan accordingly:

- unusually high levels of disk activity that occur during backups may alert an intruder
- an intruder may have installed a Trojan horse that will delete log files. An example of this occurring is that the system backup program has been modified so that if it cannot ping a router when it (the backup program) is executing, it destroys the disk. If you take the system offline and try to back it up, all logs may be lost. Refer to the practice "Eliminate all means of intruder access" for suggested ways to deal with this situation.

➤ *"Isolate" the compromised systems.*

This can be accomplished by

- transferring the backup files to a test system that is isolated from your operational systems and restoring the compromised system(s) on the test system
- disconnecting the compromised systems and performing analysis on those systems directly, keeping in mind that this will destroy the original source of information

➤ *Search on other systems for signs of intrusion.*

Intruders regularly establish more entry points into a network once they have gained initial access. Whenever an attack or an intrusion is detected, you need to check all other systems that are "similar" to the system that was accessed.

"Similar" can have various meanings depending on your operational environment, including

- systems that are in the same IP address range or are on the same network segment. Intruders perform scans across large ranges of IP addresses to locate security vulnerabilities.
- systems that are in the same "trusted" domain. These systems provide access to users from other systems within the same domain without further authentication.
- systems that have at least one network service in common. Intruders often check for well-known services such as DNS (Domain Name System), FTP (File Transfer Protocol), HTTP (Hyper-Text Transfer Protocol), and SMTP (Simple Mail Transfer Protocol).
- systems that have the same operating system

➤ *Examine logs generated by firewalls, network monitors, and routers.*

Attacks often leave trace information that can lead the analyst to the system that was used (or abused) by an intruder. Such traces include log and audit files, files left behind by an intruder, or information about the use of servers and services on other systems used in moving through the network. This trace information can be used to search for other events or connections originating from that system that were previously unnoticed. In this way, you can identify other systems to which an intruder gained access.

Firewall, network monitor, and router logs often remain intact and contain valuable information even if an intruder gains local access, manages to get administrator privileges, and deletes the local system logs to hide the information about the attack method, an intrusion itself, and the access methods used. These programs and devices, if properly configured, record connections and message traffic generated by an intruder. The logs that they each produce may reveal intruder activity. For example, firewall log files can be configured to store information about the source of any message, the destination, and characteristics of connections such as the amount of data transferred.

Using information from the analysis step above (including date, time, and systems attacked) you can locate related records in these logs that reveal more detailed information about an intrusion or information missed altogether. Look for similar connections, including connections from the same source or going to the same destination.

Building a complete picture can be a tedious task. Log formats of many systems are not compatible and no general purpose tools currently exist that chronologically synchronize logs produced by multiple systems. However, there are monitoring tools that will collect information from multiple systems and consolidate the logs produced by those systems. In addition, the timing source and time zone used by systems may differ. Protocols such as NTP (Network Time Protocol) can be used to synchronize the time for multiple systems.

➤ *Identify the attacks used to gain access to your systems.*

You should search the local logs of the compromised systems for information that reveals what kind of attack an intruder used in addition to making use of logs produced by firewalls, routers, and network monitors.

Usually, intruders attempt a number of different attacks or scan for the presence of one particular vulnerability before they gain initial access. Depending on how your systems are configured to detect signs of intrusions, your system and network logs may contain

- denied access messages if an intruder tried to guess passwords
- messages pointing to old vulnerabilities such as the UNIX sendmail "wiz" command
- blocked accesses to specific services collected by an installed tool such as TCP Wrapper

You may also find date, time, and source in the logs which can be quite useful.

After gaining access, an intruder may try to delete all logs or specific log entries. Therefore, it is possible that you will not find any useful entries. Sometimes the deletion of log entries is detectable. If so, this notifies you that something suspicious has happened to your system and you need to conduct further analysis.

➤ *Identify what an intruder did while accessing your systems.*

You need to understand how an intruder attacked and gained access to your systems. But this understanding will not reveal what an intruder actually did once access was gained. Without more information, you cannot identify what damage was done to systems and data. On many systems, you can easily identify attempts to write and modify files while, unfortunately, read access (of potentially sensitive data) is rarely captured due to the high volume of such access.

Without any further information, you should assume that once intruders gain access, they are able to obtain any data and access any service or program on the compromised system. That is, you need to assume the worst case for the purpose of assessing damage.

To identify what an intruder did, you can

- analyze various log files
- compare cryptographic checksums of known, trusted files to those on the compromised machine
- use other intrusion detection and analysis tools

Having a trusted cryptographic checksum with which to compare is particularly important to detect if an intruder modified your operating system kernel. Examples of traces intruders may leave behind include

- changes to log files to hide their presence
- actions to modify a system utility to not list processes started by an intruder to protect against easy recognition of installed back doors.
- Trojan horses, back doors, or new versions of system commands

Refer to *Detecting Signs of Intrusion* [Firth 97a] and *Preparing to Detect Signs of Intrusion* [Kochmar 98] for more information.

Policy considerations

Your organization's networked systems security policy should document the roles, responsibilities, authority, and conditions for the examination of data, systems, and for networks suspected of having been compromised and the analysis of intrusions

Your organization's information disclosure policy should indicate what information is shared with others, under which circumstances, and who has the authority to initiate information disclosure beyond that specified in your policy.

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at URL

http://www.cert.org/security-improvement/practices/p046.html

4 *Communicate with all parties that need to be made aware of an intrusion and its progress.*

Those with key roles in responding to an intrusion need to be notified and kept informed at the appropriate times to fulfill their responsibilities. You need to immediately notify the responsible mid-level and senior managers, your local computer security incident response team (CSIRT) if one exists, your public relations staff, and the affected system administrators (if they are not already involved) based on your organization's information dissemination policy. For responses to intrusions that require management approval, you need to obtain a decision about

- whether or not to close the breach and continue doing business
- whether or not to continue to gather data on an intruder's activities (including protecting evidence associated with these activities)
- what quantity and type of information you should communicate
- who you need to inform

Executing your information dissemination procedures may include contacting users affected by an intrusion, security personnel, law enforcement agencies, vendors, and other CSIRTs external to your organization.

Why this is important

The designated staff members internal and external to your organization cannot execute their responsibilities if they are not notified in a timely manner that an intrusion is occurring or has occurred and if they are not kept informed as an intrusion progresses. As a result, your systems, networks, and data may suffer greater damage (loss of confidentiality, integrity, availability) than if all those who needed to be involved had been informed as required.

Your organization may suffer loss of business or reputation if the public communication aspects of an intrusion are improperly handled.

It is important to keep communicating with other organizations about an intrusion. If they are experiencing unexpected system behavior caused by intruder actions, you may be able to gain information that will help you protect your own systems. For example, the system administrator of a site may contact you indicating that a system at your site is attacking them. An intruder may have compromised your system to hide his or her tracks and launch an attack against the other organization.

You need to initiate communication with others (e.g., managers and administrators in other parts of your organization whose systems may be vulnerable, system administrators at external customer and collaborator sites, and other CSIRTs) to identify intruder behavior that you observe. You should do this regardless of the follow-up actions you intend to take.

Be aware that communications actions may tip off an intruder causing you to alter your normal communications procedures.

It is critical that you establish and exercise your information dissemination policy and procedures before an intrusion takes place so that all parties are aware of how they are to participate when an intrusion occurs. Doing so will assist you in learning how to speak to your contacts and describe what is happening in language that is meaningful for them.

How to do It

➤ *Execute your information dissemination procedures taking the specifics of an intrusion into account.*

Establish, use, and maintain specific points of contact in support of your information dissemination policy described below (name, title, organizational affiliation, telephone number, emergency pager numbers, email address, FAX number, means of secure communication, means for authentication). Getting to know these contacts before intrusions occur helps to make your response process more efficient.

Create, use, and maintain an intrusion notification call tree (i.e., the sequence of people to call and who will call whom) and other procedures for informing people quickly. Require your intrusion response team to carry contact information with them at all times in the event they need to use it.

Share all information on a need-to-know basis and sanitize sensitive information, if required.

➤ *Use secure communication mechanisms.*

Use secure mechanisms for all communication as established and described in the practice "Prepare to respond to intrusions." Communication can be overheard or picked up by an intruder so all communication relevant to an intrusion should be done in a secure manner.

Use communications that do not involve your systems or networks such as phone and fax. Do not send email from compromised systems or networks.

➤ *Inform upstream and downstream sites of attacks and intrusions*

Upstream sites are those that were involved in an intrusion prior to your system becoming involved. Downstream sites are those that were involved after your site experienced an intrusion.

In the process of analyzing an intrusion, you are often able to gain information about systems not belonging to your organization that were

- used by an intruder to attack your systems
- attacked by an intruder from your systems
- used by an intruder to access your systems
- accessed by an intruder from your systems

Such information is usually obtained from logs about connections attributed to an intruder or from remnant files left behind by an intruder. Remnant files may include scripts with the IP addresses of the attacked hosts or the output files of attack scripts an intruder neglected to delete.

You have a responsibility to inform the administrators of all other organizations about the involvement of their systems so that they can take the necessary steps to respond to an

intrusion. This includes any ISPs that may have been involved in transmitting and receiving intruder messages. However, in the event of an ongoing legal investigation, your ability to inform other organizations may be restricted. For example, action on your part may affect the outcome of the investigation in some way or users from the other organization may, in fact, be the subject of the investigation.

➤ *Maintain a detailed contact log.*

Keep an accurate, detailed log of all contacts made and of the information exchanged.

➤ *Maintain current contact information for your systems and sites.*

Make sure your system's point of contact information in the InterNIC whois database[1] and other public directories is up to date so that other sites can contact you if they detect that your systems are involved in an intrusion at their site.

Policy considerations

Your organization's networked systems security policy should include an information dissemination policy that

- specifies who should be notified in the event of an intrusion and in what order. The order of notification may depend on the type of intrusion or other circumstances. You should contact the responsible manager, your public relations point of contact, and your local response team immediately (shown as the first, second, and third bullet items below). The remaining contacts are listed in no particular order.
  - the responsible manager and other managers who need to be made aware
  - public relations
  - CSIRT, if one exists
  - system and network administrator(s)
  - security officer and personnel
  - your site's Internet service provider (ISP)
  - human resources (in the event of an employee intruder)
  - help desk personnel (who may have to answer inquiries about an intrusion)
  - legal counsel
  - corporate investigations group, if one exists
  - law enforcement agencies (local, state, federal)
  - users
  - vendors
  - other CSIRTs external to your organization, e.g., the team associated with your ISP, CERT/CC (CERT® Coordination Center),[2] your national CSIRT
- defines specific roles and responsibilities for each contact within your organization including their range of authority
- specifies how much information should be shared with each class of contact and whether or not sensitive information needs to be removed or filtered prior to sharing it

1. Refer to http://rs.internic.net/tools/whois.html
2. CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office.

- identifies who to notify and when to notify them by using specified communication mechanisms (e.g., phone, email, fax, pager) and whether or not these mechanisms need to be secure
- who has the authority to initiate information disclosure beyond that specified in your policy

Other information

Refer to the *CSIRT Handbook* [West-Brown 98] for more information on this subject, specifically Chapter 3.7 on interactions.

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at URL

http://www.cert.org/security-improvement/practices/p047.html

5 *Collect and protect information associated with an intrusion.*

All information about the compromised system(s) and cause(s) of an intrusion needs to be captured and securely stored. This may include system and network log files, network message traffic, user files, results produced by intrusion detection tools, analysis results, system administrator console logs and notes, and backup tapes that capture the before-intrusion and after-intrusion states of the affected system. All information must be carefully collected, labelled, cataloged, and securely stored at each stage of intrusion analysis.

Why this is important

If you do not collect and protect this information, you may not be able to learn from the experience and improve your systems, their operation, and your staff capabilities. It will be difficult to interact knowledgeably with other CSIRTs. For an internally-generated intrusion, you may not be able to take appropriate action to educate, reprimand, or terminate an employee found responsible.

If you intend to prosecute an intruder, you need to have complete, thorough, and convincing evidence that has been protected through a secure chain-of-custody procedure that tracks who has been involved in handling the evidence and where it has been stored. Otherwise, the information you collect may not be considered as valid evidence in a legal proceeding. Law enforcement officials and your legal counsel are good sources for advice about how and when to collect and protect critical information.

How to do it

➤ *Collect all information related to an intrusion.*

Collect information about all relevant system and network logs from the compromised system(s), including written log records made by intrusion response staff, any other auditing information produced by tools, full backups, partial backups (snapshots), screen shots, videotapes, and photographs.

Document all information in a notebook that addresses the questions who, what, where, when, why, and how. This includes

- name of system
- date/time of each entry
- what actions were taken
- what was said
- who was notified
- who had access
- what data was collected

- what information was disseminated, to whom, by whom, when, and for what purpose
- what was submitted to legal counsel, to whom, by whom, and how it was verified (e.g., notarized)

It is important to realize that your notes may be subject to subpoena in any legal proceeding, so document responsibly. Make sure you use a separate notebook for each intrusion so if it is subpoenaed, it does not contain information about other intrusions.

➤ *Collect and preserve evidence.*

Designate a point of contact who is responsible for maintaining contact with law enforcement and other external agencies. To ensure that evidence will be acceptable to the legal community, its collection should be done following predefined procedures in accordance with all laws and legal regulations. Also do the following.

- Document, use, and maintain a procedure for preserving the compromised system and any associated evidence in case of a criminal investigation.
- Analyze a replica of a compromised resource, not the original, whenever possible, to avoid inadvertently tampering with evidence.
- Ensure that replicating the compromised resource does not change the original. This can be accomplished by write-protecting the original information prior to copying it.
- Document meticulously all actions performed by all participants from detection through analysis, response, and recovery that preserve the chain of custody (refer to the next two steps).

➤ *Ensure evidence is captured and preserved securely.*

Ensure that all log files containing information regarding an intrusion are retained for at least as long as normal business records and longer, if an investigation is ongoing.

Archive all information (listed in the previous step) to physically secure offline media.

Ensure that all critical information is duplicated and preserved both onsite at your facility and offsite in a secure location. This includes policies, procedures, contact information, tools, critical data, configurations, databases, cryptographic checksums, and system backups. Onsite alternative storage provides for quick access in the event of an emergency. Offsite storage safeguards the information in the event of a natural disaster (such as a fire or a flood).

Define and document a procedure for authorizing access to both onsite and offsite information so you can access it quickly in case of an emergency.

➤ *Preserve the chain of custody for all evidence.*

This is accomplished by having verifiable documentation indicating the sequence of individuals who have handled a piece of evidence and the sequence of locations where it was stored (including dates and times).

For a proven chain of custody to occur

- the evidence is accounted for at all times
- the passage of evidence from one party to the next is fully documented
- the passage of evidence from one location to the next is fully documented

If your organization has policy in the area of preserving and proving chain of custody, ensure that your actions are in keeping with this policy.

➤ *Contact law enforcement immediately if you decide to pursue and prosecute an intruder.*

If you choose to keep your systems running and connected to collect more information about an intruder and an intrusion (as contrasted with disconnecting or shutting down your systems), you may be liable if your system is used as a launch point to attack another site. You need to notify law enforcement immediately and take action as they advise to limit this liability.

Policy considerations

Your organization's networked systems security response procedures should ensure that a provable chain of custody is maintained for protection of potential evidence through, for example, the generation of a detailed action and decision log indicating who made each entry. This level of rigor is required even if you choose not to enter into a legal investigation with law enforcement. Other affected organizations may decide to take action and request your assistance and any evidence you have collected, and other organizations may initiate legal proceedings against you if an intruder attacked their systems from yours.

Other information

Keep in mind that laws vary from country to country. You need to determine the legal requirements of the country you are operating from (especially the laws that pertain to collecting and protecting evidence, chain of custody, and sufficiency of evidence for prosecution). Then, you need to implement the necessary procedures to meet those requirements.

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at URL

http://www.cert.org/security-improvement/practices/p048.html

6 *Apply short-term solutions to contain an intrusion.*

Containment consists of short-term, tactical actions whose purpose is to stop an intruder's access to compromised systems, limit the extent of an intrusion, and prevent an intruder from causing further damage.

Containment actions have the potential to

- quickly inform users, customers and/or business partners that an unexpected event that could affect their ability to continue their work is occurring
- alert the media that something is going on
- alert an intruder that his or her presence and activities may have been detected

Assuming you decide to contain an intrusion, your organization needs to decide whether or not to shut systems down or disconnect them from a network. These decisions require management involvement. However, if an intruder's activities are malicious, system administrators may need to take more immediate action. Therefore, the decision-making process and the level of authority need to be articulated in your security policy and made operational in your procedures.

When making decisions, you need to take into account

- an overall assessment of an intrusion (scope, impact, damage)
- any other results from the analysis such as the origin of an intruder
- your organization's goals and priorities that govern the response process
- business continuity plans

Keep in mind that any changes to the compromised systems, including containment actions, may destroy information required to assess the cause of an intrusion. You need to exercise caution to ensure that you collect all necessary data to complete the analysis before making any system changes. Also ensure that you collect and protect all evidence that may be needed in a subsequent investigation.

Why this is important

The main objectives when containing an intrusion are to

- regain control of the systems involved to be able to further analyze the problem and return the systems to normal operation
- deny an intruder access to prevent further damage and the potential for intruder interference

While an intruder still has access, you cannot ensure that you will successfully eliminate such access and be able to return your systems to normal operation. You stop intruder

access by taking containment actions. This is a short term solution. This then gives you the latitude to develop longer-term solutions once you have more detailed information.

Denying intruder access to your systems

- protects against further damage that can be caused once they realize that you have detected their presence
- prevents them from destroying valuable evidence and tampering with the system while you are analyzing it
- prevents an intruder from using your systems to attack other systems, protecting you from liability as a result of damage claims by other organizations

Containment provides a reasonable security solution until you have sufficient information to take more appropriate actions to address the vulnerabilities used to access your system and the damage done by an intruder.

How to do it

➤ *Temporarily shut down the compromised system.*

You need to temporarily shut down the compromised system when there is no other means by which to deny intruder access to the system. This action will prevent more serious damage and provide time to perform more detailed analysis. However, by doing so, you also deny access to legitimate users of the system. Therefore, we recommend that you do this only for a limited period of time, if possible.

Shutting down the compromised system may destroy important information needed for analysis. As an example, an intruder's programs may only be available in main memory as he or she deleted the files on the hard drive to avoid their detection. In an emergency, you need to be able to weigh the risk of further damage against the possibility of losing this information by shutting down.

➤ *Disconnect the compromised system from a network.*

Alternatives to shutting down a system are to

- disconnect the local area network or corporate network to which the system is connected from the local or public networks that an intruder is using
- disconnect the compromised system from the local network

The first alternative ensures that the system and all communication with it is still available from within the organization. However, this may alter critical information on the compromised system as normal use continues and will limit access to other networks for those using the disconnected network.

The second alternative allows users of systems other than the compromised system to continue to access the public network. However, if you have incorrectly determined the scope of an intrusion (that may include other systems on the same local network), you run the risk of an intruder continuing to have access to that network and the remaining systems connected to it, which may also be compromised.

➤ *Disable system services, if possible.*

If you have performed sufficient analysis to correctly limit the scope of an intrusion to specific services, you should disable them. Disabling services is especially necessary if no patch is immediately available to eliminate the vulnerability that an intruder used. By disabling only the specific services used by an intruder, you can continue to provide users on the system with access to all other services and to the system itself.

➤ *Change passwords or disable accounts.*

Although this method is not a totally reliable containment action (an intruder may have other means of access), disabling the accounts or changing the passwords associated with the accounts that an intruder is using will terminate that access path if the account was the primary means used to gain access (versus the use of a vulnerability that bypassed user authentication).

➤ *Monitor system and network activities.*

Regardless of what other steps are taken, you need to monitor all system and network activities for unusual and suspicious events. You need to watch the network for attacks previously used by an intruder and connections coming from systems known to be used by an intruder.

Using this approach, you can identify subsequent intruder access attempts more quickly and more easily. This may also reveal other access paths not previously identified which allows you to disable these access paths.

➤ *Verify that redundant systems and data have not been compromised.*

If you are running hot, warm, or cold backups in support of your configuration redundancy policy (Refer to the practice "Establish policies and procedures for responding to intrusions"), you need to ensure that an intruder's actions have not been replicated, thereby affecting those systems and data.

In addition, ensure that any containment, elimination, and restoration steps you take on the primary system are also taken on your backup systems including the elimination of vulnerabilities which were used by an intruder to gain access.

Policy considerations

Your organization's networked systems security policy should clearly state

- the acceptable level of risk to business processes and the systems and networks which support them
- to what extent business processes and the systems and networks which support them must remain operational, even in the event of intrusions or attacks
- which additional systems that reside on local networks with compromised systems will be disconnected, even if these systems are known to not (yet) be affected. This is a preventive measure.
- who is empowered to make a final decision, under which circumstances, and who has the authority to decide in situations not covered by the policy.
- how to manage password compromises, including when and how to change passwords for all users and accounts at a specific site or on an organizational level

Other Information

Recognize that there are threats (besides intrusions) that are difficult to protect against if your systems are connected to the Internet. You need to protect against damage and business impact caused by these threats in the same way you defend your system against intrusions.

You need to manage and monitor for these situations as part of your approach to risk management. Your security policy should document the actions you will take if attacks occur of the following types

- denial of service, including email bombing (sending a large volume of electronic messages to a targeted recipient until the system fails) and flood attacks (e.g., filling a channel with garbage, thereby denying others the ability to communicate across that channel or to the receiving host)
- programmed threats, such as new viruses not yet detected and eliminated by virus checking tools, or malicious applets, such as those using ActiveX and Java
- intruders scanning, probing, or mapping your systems with intent to use the results for future intrusion attempts

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at URL

http://www.cert.org/security-improvement/practices/p049.html

7 *Eliminate all means of intruder access.*

Complete eradication of the root cause(s) of an intrusion is a long-term goal that can only be achieved by implementing an ongoing security improvement process. In response to a specific intrusion, you need to ensure that the affected systems are protected against the same or similar types of access and attacks in the future, once an intrusion is contained and systems are returned to normal operation.

As part of a successful intrusion, intruders typically install back doors or other means for obtaining future access to the compromised system. This practice describes steps to eliminate this access to the greatest possible extent. These steps are likely sufficient if you have prepared properly[1], performed thorough analysis[2], and if you are able to identify all changes made by an intruder.

If you are not prepared, then your only option is to reinstall the systems and restore all user data to the extent possible. Many administrators may choose to reinstall the systems in any event to ensure that all intruder changes are eliminated or because they doubt the accuracy of the information they are relying on to identify such changes.

Why this is important

Intruders widely advertise compromised systems and regularly trade system addresses and access information in exchange for attack tools or similar information. Victims of intrusions indicate that intruders try to access their system addresses long after the original intrusion has occurred. Such addresses are not only distributed amongst intruders but also are available in databases accessible on the Internet.

You need to ensure that your systems are no longer vulnerable before returning them to service. Otherwise, they can be compromised by the same kind of attack that resulted in the successful intrusion. The absence of elimination actions undermines your ability to operate securely and, in effect, negates all efforts you expend to respond to the original intrusion.

How to do it

➤ *Change all passwords on all systems to which the attacker may have had access.*

While we recommend that this step be taken in all cases, it is most important when there is evidence that an intruder may have had access to your password file or used a password sniffer tool that captures user passwords transmitted in clear text on the network.

You need to plan for the fact that executing and enforcing this step will create a fair

1. Refer to the practice, "Prepare to respond to intrusions."
2. Refer to the practice "Analyze all available information to characterize an intrusion."

amount of work for users and may confuse them. If passwords cannot be changed, another alternative is to lock out the compromised accounts and reassign new accounts.

➤ *Reinstall compromised systems if your preparation was insufficient.*

If you are insufficiently prepared, you likely do not have access to information such as cryptographic checksums to verify the authenticity of the operating system version used on the compromised systems. In this event, you need to reinstall these systems from the original distribution media or from copies you trust.

After successful reinstallation of the operating system, you need to reinstall site-specific modifications to your systems, apply all relevant patches and bug-fixes, and ensure that these modifications do not introduce additional defects or vulnerabilities. One possible means for doing so is to execute a known series of system regressions tests if you have such a set of tests and prior test results are available for comparison.

➤ *Remove any means for intruder access including changes made by an intruder.*

Use the results of the analysis of an intrusion to determine the means by which an intruder gained access and eliminate them. Examples include

- known vulnerabilities for which patches are available; install the patches
- the presence of malicious code (back door, Trojan horse) with an unknown and hidden function such as deleting log files or starting a service on unused ports to permit access without requiring a password; reinstall a trusted version of the affected software
- adding new users to the list of authorized users including levels of system privileges up to full privileges; reinstall a trusted version of your authorized users file
- setting new passwords for existing users; reinstall a trusted version of your password file
- weak or inadequate procedures (e.g., password setting and aging); update the procedures and enforce them
- corrupted configuration files containing, e.g., previously disabled entries (such as a rshd daemon entry within the inetd.conf configuration file on UNIX systems); correct them
- inspect all files executed at boot time for the presence of Trojan horses or back doors; reinstall a trusted version of file executed at boot time

➤ *Restore executable programs (including application services) and binary files from original distribution media.*

You need to identify all files that have been added, changed, or deleted by an intruder because you cannot determine what hidden functions may have been left behind or what critical functions may have been influenced by these changes. For executable files (including non- binary files such as UNIX shell scripts) and other binary files (such as libraries), verify cryptographic checksums to ensure that the files were not compromised. Refer to the practice, "Generate information required to verify the integrity of your systems and data," in *Preparing to Detect Signs of Intrusion* [Kochmar 98].

Possessing detailed logging or audit information about files an intruder accessed and programs an intruder executed makes this step much easier by allowing your staff to concentrate on specific files instead of all existing and deleted files.

➤ *Review system configurations.*

System configuration files include the following types of data

- user accounts
- system services and their configuration
- audit and monitoring facilities
- access control lists

Compare all system configuration files with authoritative copies of these files or compare cryptographic checksums with trusted checksums collected before an intrusion.

If authoritative copies are available, you may choose to overwrite the current set of files with these copies.

In the absence of trusted copies or checksums, you need to review all files manually. Clearly, this will take significant time and resources. The review can be effectively conducted as a peer review performed by multiple system and network administrators or by members of your response team.

➤ *Determine if you have uncorrected system and network vulnerabilities and correct them.*

Particularly attend to vulnerabilities for which exploit scripts and tools exist within the intruder community and where vendor solutions are available as patches or hot-fixes.

You can conduct a security audit or evaluation of your systems by executing public domain or vendor tools (such as SATAN for UNIX systems) or arrange for external experts to check for the presence of known vulnerabilities.

➤ *Improve protection mechanisms to limit the exposure of networks and systems.*

All protection mechanisms (such as firewalls) should be reviewed and their configurations adjusted based on what you learn in responding to a successful intrusion. Pay particular attention to the following aspects.

- Determine if protection mechanisms need to be configured differently (such as changing or adding new IP addresses to the router filter for allowing or disallowing connections).
- Determine if protection mechanisms need to be placed in a new or additional location on your network that was previously unprotected or insufficiently protected.
- Review available information on vulnerabilities, patches, and new versions of your protection mechanism software, ensuring that your configurations are up to date.

➤ *Improve detection mechanisms to enable better reporting of attacks.*

Update your detection mechanisms, such as intrusion detection systems and other types of intrusion reporting tools, to ensure that similar attacks are detected by these mechanisms in the future. Perform the following analysis and take appropriate actions.

- Determine if detection mechanisms need to be configured differently (such as adding in new attack patterns to be detected, or changing logging options).
- Determine if detection mechanisms need to be placed in a new or additional location on your network that was previously insufficiently covered.
- Review available information on vulnerabilities, patches, and new versions of your detection mechanism software, ensuring that your configurations are up to date.
- Review and update the conditions under which your detection mechanisms generate

alerts to system and network administrators and the forms in which the alert is made (e-mail, phone, pager, printouts, etc.).

Refer to *Preparing to Detect Signs of Intrusion* [Kochmar 98] for help identifying logging approaches and tools that you may want to add. The practice "Establish a policy and procedures that prepare your organization to detect signs of intrusion" and its supporting implementation on sources of additional information are especially helpful.

Policy considerations

Your organization's networked systems security policy should require

- regular checks for the presence of system and network vulnerabilities
- timely evaluation and selective installation of patches and other corrections that you need to operate securely
- that you stay informed about the constantly changing sequence of new alerts, security bulletins, and advisories, particularly as they affect your protection and detection mechanisms. This can be very resource-intensive, so you need to be selective regarding information sources that you review regularly.
- that roles and responsibilities are clearly assigned within your organization to perform regular checks, install patches, and to stay current with new information
- that password transmission across an untrusted network be protected by encrypting passwords or by using other secure authentication technologies such as one-time passwords using challenge-response approaches or security tokens

Other information

Refer to *Preparing to Detect Signs of Intrusion* [Kochmar 98] and *Detecting Signs of Intrusion* [Firth97a] for further guidance on tools and approaches that support this practice, especially steps related to the detection of changes made by an intruder.

Implementations specific to a given operating system are available at http://www.cert.org/security-improvement.html.

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at URL

http://www.cert.org/security-improvement/practices/p050.html

8 *Return systems to normal operation.*

Restoring and returning a compromised system to normal operation permits your staff to have access to that system again. This is best accomplished after all means of intruder access are eliminated. Doing so prevents the same or similar types of intrusions from occurring or, at the very least, ensures timely detection and notification by your updated intrusion detection mechanisms.

Business reality may require that you return systems to operation before full intrusion analysis is completed and all corrections are made. This risk needs to be carefully managed and monitored. If this is the case, you need to continue analysis and eliminate an intruder's access to your system as soon as possible, recognizing that your system is vulnerable to another occurrence of the same type of intrusion. Containing an intrusion becomes even more critical.

The purpose of this practice is to define steps to help you correct damage caused by an intruder or caused by the actions taken to contain an intrusion, such as disconnecting the compromised systems from your network. Details about restoring any specific business application or related service are beyond the scope of this practice but these steps can be used in those cases as well.

Why this is important

One of the purposes of a having a response process is to eliminate vulnerabilities that allowed an intrusion to occur and to return affected systems to full operational status. If these systems cannot be successfully reinstated, the business operations that depend on them cannot be performed. The efforts to eliminate intruder access and analyze intruder activities to determine vulnerabilities are wasted if systems cannot be returned to service.

How to do it

➤ *Determine the requirements and timeframe for returning the system to normal operations.*

You need to fully determine the requirements to be met and the priority they should have before you return the affected system to normal operations. This determination requires the involvement of senior management.

If the requirements do not include completion of intrusion analysis and the elimination of vulnerabilities (due to a business-critical need to return the system to operations as soon as possible), continue analysis in parallel and upgrade the system as soon as possible, recognizing that the system is vulnerable to another occurrence of the same type of intrusion until you do so. One way to mitigate the risk is to increase the level of monitoring and intrusion detection to ensure that a new intrusion does not go unnoticed.

➤ *Restore user data from trusted backup media*

An intruder may have altered user data and application program areas.
Examples where this may occur include

- installing back doors to provide future access. For example, an intruder installs a program in a local user directory that is called each time the user logs in, providing an unprotected login shell that can be accessed by anyone via the Internet.
- compromising user data to sabotage the user's work. For example, an intruder makes small changes to spreadsheets that go unnoticed. Depending on how the spreadsheets are used, this can cause minor to major damage.

Use the latest trusted backup to restore user data. For files that have not been compromised, you can consider using the backup that was made closest in time to when an intrusion was detected to avoid user rework. This should be done with caution and is based on having a high level of confidence that restored user files were not compromised. Regardless, you need to encourage users to check for any unexpected changes to their files and warn them about the risk of compromise.

Users should review all restored data files that resided on the compromised system to ensure they were not affected by an intruder's activities.

All executables or binary files residing in user areas should be handled in the same way as system executables and binary files. If no authenticated, cryptographic checksum is available, you need to reinstall from the original distribution media.

➤ *Enable system and application services.*

Enable previously disabled services that are either known as not vulnerable or have been corrected to eliminate the vulnerability used by an intruder.

Only enable those services that are required by the users of the system (as contrasted with enabling all available services).

➤ *Reconnect the restored system to the network.*

Reconnect the restored system to its local network. In the case where a local or corporate network containing the compromised system was previously disconnected from the public network used by an intruder, reconnect the local or corporate network.

➤ *Validate the restored system.*

Validate the restored system executing a known series of regression tests where prior test results are available for comparison.

➤ *Watch for additional scans or probes that may signal the return of an intruder.*

In many cases, you can gather much more information about an intruder when they attempt to return than you can immediately after an intrusion. This is particularly true if you have installed improved monitoring tools and procedures as a result of lessons learned from a previous intrusion.

Monitor for failed login attempts, attempts to access back doors, attempts to re-exploit the original vulnerability, and attempts to exploit new vulnerabilities. Each occurrence of these should be analyzed further.

Once a system is compromised and this becomes known in the intruder community, the system becomes a bigger target for future attacks. Improved monitoring may reveal new attacks more easily and provide the opportunity to defeat the attacker.

Policy considerations

Your organization's networked systems security policy should specify the order in which system services are returned to operation. This is to ensure that the order meets your business objectives and priorities while minimizing impact on users, when possible.

Actions to restore any specific business application or related service should be taken as recommended above for restoring systems after an intrusion.

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at URL

http://www.cert.org/security-improvement/practices/p051.html

9 *Identify and implement security lessons learned.*

It is important to learn from the successful and unsuccessful actions taken in response to an intrusion. Capturing and disseminating what worked well and what did not will help reduce the likelihood of similar intrusions and will improve the security of your operation. This can be accomplished by performing a post mortem review with all involved parties and communicating the results of the review.

There are several additional tasks that need to be performed in the aftermath of an intrusion. These include notifying any individuals or teams with whom you have been communicating about the outcome of an intrusion and putting in place monitoring mechanisms and security policy and procedure updates resulting from knowledge gained through the lessons learned process.

Why this is important

If your organization does not learn from the experience of responding to a successful intrusion, you will continue to operate at risk and will likely have to deal with the same or a similar type of intrusion again. Every successful intrusion indicates weaknesses in your systems, networks, and operations that provide opportunities to make them more secure. It may also point to an inadequate level of staff preparedness that can be remedied through additional training or other forms of skill development.

How to do it

➤ *If further notification is required (per policies and procedure), execute this notification.*

Follow up with the sites you contacted previously.

➤ *Manage ongoing press aspects of an intrusion, if any.*

Do this in accordance with your information dissemination policy. Refer to the practice "Communicate with all parties that need to be made aware of an intrusion and its progress."

➤ *Hold a post mortem analysis and review meeting with all involved parties.*

Do this within three to five working days of completing the investigation of an intrusion. Otherwise, participants are likely to forget critical information.

Capture the following information.

- Did your detection and response processes and procedures work as intended? If not, where did they not work? Why did they not work?
- methods of discovery and monitoring procedures that would have improved your ability to detect an intrusion

- improvements to procedures and tools that would have aided you in the response process. For example, consider using updated router and firewall filters, placement of firewalls, moving the compromised system to a new name or IP address, or moving the compromised machine's function to a more secure area of your network.
- improvements that would have enhanced your ability to contain an intrusion
- correction procedures that would have improved your effectiveness in recovering your systems
- updates to policies and procedures what would have allowed the response and recovery processes to operate more smoothly
- topics for improving user and system administrator preparedness
- areas for improving communication throughout the detection and response processes

Make a monetary estimate of the costs associated with an intrusion to support the business case for the level of investment you should make in security improvement. This should include the estimated value of proprietary or sensitive information assets that may have been accessed by an intruder.

Document and review meeting results.

Prepare a final report and brief these results to senior management (CIO/CEO level) for their review and comment. This ensures they are aware of the vulnerability of their systems and continue to be educated about these issues.

➤ *Revise security plans, policies, procedures, and user and administrator training to prevent intrusion recurrence.*

Include any new, improved methods resulting from lessons learned in your current security plan, policies, and procedures.

Make sure that you are regularly reviewing the public, legal, and vendor information sources necessary to protect your systems from further attacks of this type. These sources regularly report current intruder trends, new attack scenarios, and tools that will improve the effectiveness of your response process.

Refer to the supporting implementation "Maintaining currency by periodically reviewing public and vendor information sources" in *Preparing to Detect Signs of Intrusion* [Kochmar 98].

➤ *Determine whether or not to perform a new risk analysis based on the severity and impact of an intrusion.*

➤ *Take a new inventory of your system and network assets.*

Refer to the practice "Generate information required to verify the integrity of your systems and data" in *Preparing to Detect Signs of Intrusion* [Kochmar 98].

➤ *Participate in investigation and prosecution, if applicable.*

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at URL

http://www.cert.org/security-improvement/practices/p052.html

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	February 1999	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Responding to Intrusions	C — F19628-95-C-0003

6. AUTHOR(S)

Klaus-Peter Kossakowski, Julia Allen, Christopher Alberts, Cory Cohen, Gary Ford, Barbara Fraser, Eric Hayes, John Kochmar, Suresh Konda, William Wilson

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

8. PERFORMING ORGANIZATION REPORT NUMBER

CMU/SEI-SIM-006

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

HQ ESC/DIB
5 Eglin Street
Hanscom AFB, MA 01731-2116

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12.a DISTRIBUTION/AVAILABILITY STATEMENT	12.b DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (maximum 200 words)

Most organizations are not adequately prepared to deal with intrusions. They are likely to address the need to prepare and respond only after a breach occurs. The result is that when an intrusion is detected, many decisions are made in haste and can reduce an organization's ability to

- understand the extent and source of an intrusion
- protect sensitive data contained on systems
- protect the systems, the networks, and their ability to continue operating as intended
- recover systems
- collect information to better understand what happened. Without such information, you may inadvertently take actions that can further damage your systems.
- support legal investigations

Even if you have sophisticated prevention measures in place, intrusions can happen. In this module, we describe practices to be implemented independent of the size, type, or severity of an intrusion or of the methods used to gain access. The key event is that an intruder has gained access to your systems or data.

You need a strategy for handling intrusions effectively that includes preparation, detection, and response. The practices in this module identify steps you must take to respond to and recover from a detected intrusion.

This module is a companion module to CMU/SEI-SIM-005 *Preparing to Detect Signs of Intrusion* and CMU/SEI-SIM-001 *Detecting Signs of Intrusion.*

14. SUBJECT TERMS	15. NUMBER OF PAGES
breakin, security, intrusion detection, computer security	56
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL